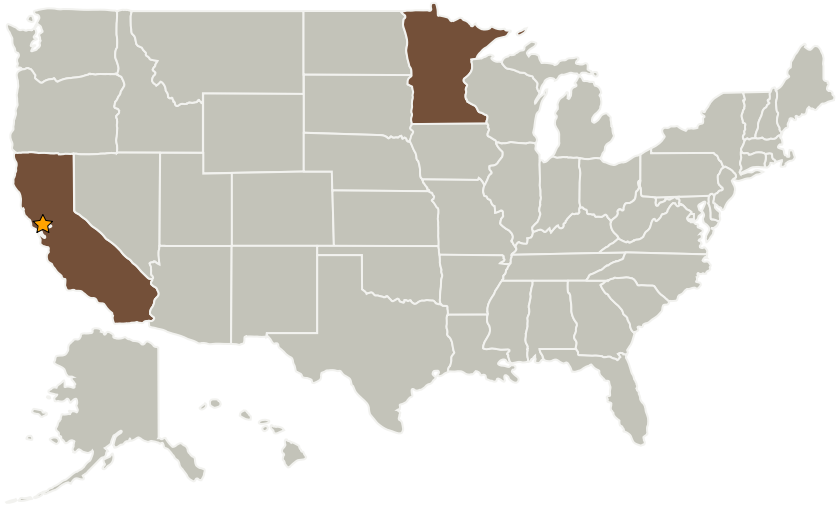
SAFE-P: System for Assurance of Flight Executable Procedures, Phase I

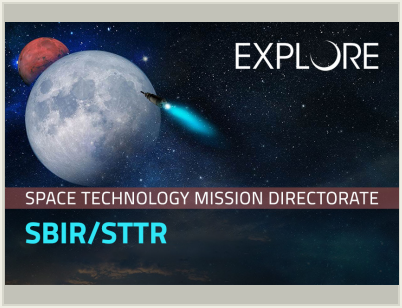
Completed Technology Project (2009 - 2009)

Project Introduction

Problem: Ensuring that command execution scripts do not deviate from Standard Operating Procedures (SOPs) is time-consuming, costly, and error-prone. Deviations can be inefficient or hazardous. Solution: We propose to design and develop SAFE-P, an interactive tool to ensure conformance between command scripts and procedures, or guide users to clarify their rationale for deviations. Using semantic differencing and formal verification of bisimulation relations, SAFE-P will ensure that the scripts comply with SOPs and will highlight differences for the operators, so that they can double-check their work and confirm any deviations from standard procedures. SAFE-P's design will begin with relatively simple syntactic mechanisms to find differences between command sequences and textual procedures that can be applied directly to current flight control practices, including the use of SOPs captured in simple XML or PDF files and command scripts in ThinLayer. To reduce false error detection and assess the criticality of differences, we will incorporate knowledge of the space platform's architecture. For future missions, we will extend SAFE-P to richer languages (PRL, PLEXIL, SCL) and employ more complex verification of program-equivalence relationships (bisimulation) to ensure conformance between scripts and procedures.

Primary U.S. Work Locations and Key Partners





SAFE-P: System for Assurance of Flight Executable Procedures, Phase I

Table of Contents

Organizational Responsibility

Responsible Mission Directorate:

Space Technology Mission Directorate (STMD)

Lead Center / Facility:

Ames Research Center (ARC)

Responsible Program:

Small Business Innovation Research/Small Business Tech Transfer

Small Business Innovation Research/Small Business Tech Transfer

SAFE-P: System for Assurance of Flight Executable Procedures, Phase I

Completed Technology Project (2009 - 2009)

Organizations Performing Work	Role	Type	Location
★Ames Research Center(ARC)	Lead Organization	NASA Center	Moffett Field, California
SIFT, LLC	Supporting Organization	Industry	Minneapolis, Minnesota

Primary U.S. Work Locations	
California	Minnesota

Project Management

Program Director:

Jason L Kessler

Program Manager:

Carlos Torrez

Technology Areas

Primary:

- TX11 Software, Modeling, Simulation, and Information Processing
  - TX11.1 Software Development, Engineering, and Integrity
    - TX11.1.5 Architecture and Design of Software systems